

11/30/06

n. 218 #67, 10
n. 282 #23/8

Def Let R be a commutative ring, $a, b \in R$ and $b \neq 0$.

1. Say b divides a if $a = bx$ for some $x \in R$. (a is a multiple of b)
Write $b|a$.
2. A greatest common divisor of a & b is $a \neq 0, d$ such that
 - $d|a, d|b$
 - If $e|a, e|b$ then $e|d$.

Write (a, b)

Prop

1. $b|a$ iff $(a) \subseteq (b)$
2. Thus $(a, b) \subseteq (d)$ where $d = \text{gcd}(a, b)$.
3. Suppose the ideal (a, b) is principal (d) . Then d is a gcd.

* If R is not a PID then (a, b) may not be principal.

e.g. $\mathbb{Z}[x], \text{gcd}(2, x) = 1$

but $(2, x) \neq (1)$.

Prop Let R be an integral domain. Then two different gcd's differ by a unit.

Proof Let d, d' be gcd's. Then $d = xd', d' = yd$ so $d = xyd$

$$d(1-xy) = 0 \quad xy = 1.$$

Remarks

1. gcd's may not even exist.
2. When they do exist, may be hard to find!

Theorem Suppose R is Euclidean Domain, $a, b \in R - 0$.
Let $d = r_n$ be last nonzero remainder. Then

1. d is a gcd of (a, b)

2. (a, b) is principal, $(a, b) = (d)$,

In particular $d = ax + by$.

Proof

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$$\vdots$$

$$r_{n-2} = q_{n-1} r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} r_n$$

Recall that $ED \Rightarrow PID$ so (a, b) is principal, i.e. \exists a gcd d . So:

1. $r_n \mid a, r_n \mid b$ so $(a, b) \mid (r_n)$

2. $r_n = ax + by$ so $(r_n) \in (a, b)$

Proof 1 Just trace back $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-2} \Rightarrow \dots$

Proof 2 Other way

$r_0 \in (a, b) \Rightarrow r_1 \in (a, b) \Rightarrow \dots \Rightarrow r_n \in (a, b)$

Example 273 and 2310

$$2310 = 8 \cdot 273 + 126$$

$$273 = 2 \cdot 126 + 21$$

$$126 = 6 \cdot 21$$

Thus $21 = (273, 2310)$

$$21 = 273 - 2 \cdot 126$$

$$= 273 - 2 \cdot (2310 - 8 \cdot 273) = 17 \cdot 273 - 2 \cdot 2310$$

Remark This finds gcd's in \mathbb{Z} very fast $\approx \log n$.

Conclusion: In a Euclidean Domain gcd's exist and can be found.

PID's

Prop Let $a, b \in \text{PID } R$.

1. a, b have a gcd d where $d = (a, b)$.
2. Thus $d = ax + by$, some $x, y \in R$.
3. d is unique upto mult by units.

Proof We already showed that $(a, b) = (d) \Rightarrow d$ is a gcd.

Prop In a PID, maximal ideal \iff prime ideal.

Proof Recall maximal \Rightarrow prime.

So let (p) be prime. Suppose $(a) \subset (m) \subset R$. Then

$p = rm$, so $r \in (p)$ or $m \in (p)$. So let $r \in (p)$.

Then $r = ps$ so $p = psm$ so $sm = 1 \neq$

Q: We know E.D \Rightarrow P.I.D, converse?

4

Def A positive norm N is Dedekind-Hasse if

$\forall a, b \in R - 0$ either

1. $a \in (b)$

2. $\exists s, t \in R$ with $0 < N(sa - tb) < N(b)$

Rmk \mathbb{Z} is Euclidean.

Prop R is a P.I.D iff it has a D-H norm.

Proof \Leftarrow

Let I an ideal. Choose $b \in I$ minimal norm.

Let $a \in I$ with $a \notin (b)$. Then $sa - tb$ gives $*$

\Rightarrow later.

Rmk This is just the same proof that E.D \Rightarrow P.I.D

COR

$\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a P.I.D but not a E.D.

Pf

$$N(a + b \left[\frac{1 + \sqrt{-19}}{2} \right]) = a^2 + ab + 5b^2$$

UFD's

Def R an integral domain

1. $r \neq 0$ is irreducible if not a unit
and $r = ab \Rightarrow a$ or b a unit.
2. $p \neq 0$ is prime if $p|ab \Rightarrow p|a$ or $p|b$
(Equiv (p) is prime)
3. a, b are associates if $a|b$ and $b|a$.

Lemma In an I.D. associates differ by a unit.

Prop In I.D. prime \Rightarrow irreducible.

Prop In a PID prime \Leftrightarrow irred.

Example $2 \in \mathbb{Z}/6\mathbb{Z}$ is prime,
Not irred.

Example In $\mathbb{Z}[\sqrt{-3}]$ 3 is irreducible but
Not prime!

Proof $(1 + \sqrt{-3}) | (1 - \sqrt{-3}) \Rightarrow 6 \in (3)$

Define UFD.